Amendments to the Claims: This listing of claims will replace all prior versions, and listings, of claims in the application

Listing of Claims:

1. -14. (Canceled)

15. (Original) A method for identifying an encryption value in a Finite field, F_P, where P is a prime number, based on a private key PV and a received public key PB, comprising the steps of:

determining a mathematical inverse of PB modulo P by performing the steps of:

a) assigning P to a temporary variable U and assigning PB to a temporary variable V and assigning a value of zero to a temporary variable U2 and assigning a value of one to a temporary variable V2;

b) selecting 2M most significant bits of U as a first value U_{2M} and selecting 2M most significant bits of V as a second value V_{2M}, dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

c) determining a value T as U minus the quantity Q times V;

d) if T is less than zero, applying a correction term to Q to obtain a corrected value Q' and assigning the new value for T as U minus the quantity Q' times V;

e) determining a value T2 as U2 minus Q times V2, assigning the value in V2 to U2, assigning the value T2 to U2, assigning V to U and T to V; and

f) repeating steps a) through e) until V equals zero, whereby the value remaining in U2 is the mathematical inverse of PB; and

dividing PV by PB modulo P by multiplying PV times the mathematical inverse of PB, wherein the result is the encryption value.

16. (Original) A method according to claim 15, wherein:

step d) includes the step of selecting 2M most significant bits of T to define a value T_M, wherein the step of applying the correction term is given by the equation:

$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1)$; and

step d) further includes the step of calculating Q", a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

17. (Original) A method according to claim 15, wherein the variable U has a most significant bit at bit-position B1 and the variable V has a most significant bit at bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method further including the steps of:

subtracting B2 from B1 to obtain a difference value D;

comparing D to a predetermined threshold value wherein steps a) through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e) performing the steps of:

determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M;

assigning a new value to U as U times X plus Y times V and determining the value T2 as X times U2 plus Y times V2; and

switching the values of U and V and assigning the value of V2 to U2 and assigning the value T2 to U2.

18. (Original) A method according to claim 17, wherein the step of determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M, includes the step of invoking a further GCD routine.

19. (Original) A method according to claim 17, wherein 2M equals 32 and the further GCD routine is a Euclid routine having a modified termination condition.

20. (Original) A method according to claim 17, wherein 2M equals 64 and the further GCD routine is a Lehmer routine having a modified termination condition.

21. (New) A method for identifying an encryption value in an elliptic curve cryptographic system, the method comprising the steps of:

Calculating the encryption value, (x3, y3), according to the equation

(x1, y1) + (x2, y2) = (x3, y3), where

$x3 = L^2 - x1 - x2$; $y3 = L (x1 - x3) - y1$ and $L = (y1 - y2) / (x1 - x2)$, where (x1, y1) and (x2, y2) represent input values to the elliptic curve cryptographic system and L is an intermediate value, wherein the method includes the step of

determining a mathematical inverse of (x1 - x2) modulo a prime number by performing the steps of:

a) assigning the prime number to a temporary variable U and assigning a first calculated value, (x1 - x2), to a temporary variable V and assigning a value of zero to a temporary variable U2 and assigning a value of one to a temporary variable V2;

b) selecting 2M most significant bits of U as a first value U_{2M} and selecting 2M most significant bits of V as a second value V_{2M}, dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

c) determining a value T as U minus the quantity Q times V;

d) if T is less than zero, applying a correction term to Q to obtain a corrected value Q′ and assigning the new value for T as U minus the quantity Q′ times V;

e) determining a value T2 as U2 minus Q times V2, assigning the value in V2 to U2, assigning the value T2 to U2, assigning V to U and T to V; and

f) repeating steps a) through e) until V equals zero, whereby the value remaining in U2 is the mathematical inverse of the first calculated value; and

dividing a second calculated value, (y1 + y2), by the first calculated value modulo the prime number by multiplying the second calculated value times the mathematical inverse of the first calculated value to obtain the intermediate value, L.

22. (New) A method according to claim 21, wherein:

step d) includes the step of selecting 2M most significant bits of T to define a value T_M, wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1); \text{ and}$$

step d) further includes the step of calculating Q″, a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

23. (New) A method according to claim 21, wherein the variable U has a most significant bit at bit-position B1 and the variable V has a most significant bit at bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method further including the steps of:

subtracting B2 from B1 to obtain a difference value D;

comparing D to a predetermined threshold value wherein steps a) through d) are performed only if D is greater than a predetermined threshold value;

if D is not greater than the predetermined threshold, then, before step e) performing the steps of:

determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M;

assigning a new value to U as U times X plus Y times V and determining the value T2 as X times U2 plus Y times V2; and

switching the values of U and V and assigning the value of V2 to U2 and assigning the value T2 to U2.

24. (New) A method according to claim 23, wherein the step of determining values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M, includes the step of invoking a further GCD routine.

25. (New) A method according to claim 23, wherein 2M equals 32 and the further GCD routine is a Euclid routine having a modified termination condition.

26. (Newly Added) A method according to claim 23, wherein 2M equals 64 and the further GCD routine is a Lehmer routine having a modified termination condition.